UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	Case No.: 1: 18 CR 22
	)	
Plaintiff	)	
	)	
v.	)	JUDGE SOLOMON OLIVER, JR.
	)	
PHILLIP DURACHINSKY,	)	
	)	
Defendant	)	ORDER

Currently pending before the court in the above-captioned case is Defendant Phillip Durachinsky's ("Defendant") Motion to Suppress (ECF No. 63). For the following reasons, the court denies Defendant's Motion.

I. Background

On January 4, 2017, Case Western Reserve University ("CWRU") discovered that its computer network likely was compromised by malware, which came to be known as "Fruitfly." (Mot. to Suppress at PageID #237–38, ECF No. 63.) CWRU contacted the Federal Bureau of Investigation ("FBI") the next day and identified over one hundred infected computers on its network. (*Id.*) They also determined that the malware originated as early as 2013. (*See* Macfarlane Aff. at PageID #309–10, ECF No. 63-2; Ex. to Resp. in Opp'n at PageID #390, ECF No. 66-1.)

CWRU subsequently determined that an IP address associated with Fruitfly had also been used to access the email account of CWRU alumnus Defendant Phillip Durachinsky. (Mot. to Suppress at PageID #238, ECF No. 63.) At that point, Defendant became the primary target of the FBI investigation. (*Id.*) On January 10, 2017, the FBI conducted a background check on Defendant

and examined his Bureau of Motor Vehicle records. (*Id.*) In response to the FBI's subpoena, AT&T provided subscriber information showing that the suspected IP address pointed to a residential address in North Royalton, Ohio, where Defendant lived with his parents. (*Id.*)

Several subsequent events accelerated the investigation. On or about January 6, 2017, victims of Fruitfly began to remediate their networks. The Government asserts that at least some of this activity would have been detectable by Defendant. (Resp. in Opp'n at PageID #360.) On January 13, 2017, Fruitfly changed to a new IP address that pointed to a location in California. (*Id.* at PageID #360–61) Then, on January 18, 2017, two articles appeared online reporting Fruitfly, its new IP address, and a forthcoming security update from Apple. (Ex. to Resp. in Opp'n at PageID #388–94, ECF No. 66-1.) It is unclear whether Defendant knew about these articles or the remediation efforts. Nonetheless, the FBI agents worried that critical evidence would be destroyed as Apple issued its corrective software patch or Defendant dismantled Fruitfly to cover his tracks. (Resp. in Opp'n at PageID #360–61, ECF No. 66.)

Despite the agents' concerns and the evidence mounting against Defendant, they did not immediately seek a warrant because the United States Attorney's Office in Cleveland and the Department of Justice in Washington, D.C., determined that additional legal process was necessary. (*See id.* at PageID #361–62.) Instead, the FBI agents decided to approach the Durachinsky's to ask for consent to search their home and computer equipment. Before going to the home, the agents made preliminary arrangements with the Magistrate Judge on duty to submit a search warrant later that night. (*Id.*)

The FBI conducted a "knock and talk" at Defendant's home at approximately 10:00 p.m. on January 18, 2017. (Mot. to Suppress at PageID #238, ECF No. 63.) Three FBI agents initially approached the house: Special Agent Macfarlane ("SA Macfarlane"), Special Agent Brian ("SA Brian"), and Special Agent Florence ("SA Florence"). Defendant was at work, but his father ("Mr.

Durachinsky") answered the door and allowed the agents inside. (*Id.*) Defendant's mother ("Mrs. Durachinsky"), who had been in bed, got up and joined them in the kitchen, where the agents explained they were investigating suspicious network activity that originated from the Durachinsky's home IP address. (*Id.* at PageID #239.) During this conversation, two additional members of the investigation team, Special Agent Hantz ("SA Hantz") and Computer Scientist Corrigan ("CS Corrigan"), also entered the home.

At the FBI agents' request, Mr. and Mrs. Durachinsky let the agents search their personal computers. Mr. Durachinsky signed a consent to search form for his HP desktop computer and led agents to the basement to inspect it. (Mot. to Suppress at PageID #239, ECF No. 63.) Likewise, Mrs. Durachinksy signed a consent form for her Dell laptop, which was in the living room. (*Id.*) CS Corrigan testified that he examined these computers and quickly determined they were not involved with Fruitfly.

The agents then asked if there were other computers in the house, and Mrs. Durachinsky responded that Defendant kept a laptop in his computer room. She also told the agents that Defendant stayed at the house only part time, but that he was "very smart regarding computers" and could remotely access the laptop from work. (Resp. in Opp'n at PageID #363.) Defendant's parents then led the agents to the computer room, opened the door, and pointed to an ACER Aspire laptop sitting on the desk. (Mot. to Suppress at PageID #240, ECF No. 63.)

Apparently, Defendant's parents returned to the kitchen with SA Florence while other agents and CS Corrigan stayed in the computer room. Defendant's parents admitted that Defendant had been disciplined in high school for hacking into his teachers' email accounts. (Resp. in Opp'n at PageID #363.) Yet Mrs. Durachinsky also testified that she repeatedly told the agents they had to get Defendant's consent before searching his laptop. Accordingly, at SA Florence's request, Mrs.

Durachinsky attempted to contact Defendant and left a voicemail with one of his coworkers. (*See* Mot. to Suppress at PageID #242, ECF No. 63.)

Meanwhile, CS Corrigan and the agents began to examine Defendant's laptop. The Government claims that, upon entering the computer room, "CS Corrigan noticed the laptop lid was slightly open and observed the mouse pointer was moving and the screen was updating." (Macfarlane Aff. at PageID #313–14, ECF No. 63-2.) Worried that "someone was remotely accessing the laptop" and destroying evidence, CS Corrigan opened the laptop fully and unplugged the ethernet cable while SA Brian disconnected the wireless router in the basement. (Resp. in Opp'n at PageID #364, ECF No. 66.) However, Defendant challenges this version of events, arguing that his computer expert and the FBI's own technical report show the laptop was closed when the agents arrived. (Mot. at PageID #243–44, ECF No. 63.) The Government responds that the state of the lid is irrelevant because, even if it was closed, the circumstances allowed CS Corrigan to open the laptop and examine it. (Resp. in Opp'n at PageID #373–74 n.7, ECF No. 66.) At any rate, the agents' actions terminated any remote connection that had been active and revealed a screen displaying evidence of malware.

Back in the kitchen, Mrs. Durachinsky received a call from Defendant shortly after SA Brian disconnected the router. (*Id.* at PageID #364.) Mrs. Durachinsky passed the phone to SA Florence, who explained the situation and asked Defendant for consent to search his laptop. When Defendant repeatedly refused, SA Florence responded that the agents could seize the laptop immediately due to exigent circumstances and that they would subsequently obtain a search warrant. (Resp. in Opp'n at PageID #364.)

The agents in the computer room began the seizure process in accordance with the FBI's procedures for electronic evidence. (*See* Resp. in Opp'n at PageID #373–74 n.7, ECF No. 66) They took photos and videos of the various programs that were open on the laptop's screen to preserve

evidence, and CS Corrigan entered commands on the keyboard to test for encryptions that would lock or erase data. (*See id.* at PageID #365 n.4, 373–74 n.7.) Finding none, the agents seized Defendant's laptop and a nearby Western Digital external hard drive at approximately 10:55 p.m. (*Id.* at PageID #364.) CS Corrigan testified that he later entered additional commands on the laptop in another check for encryptions after he returned to FBI headquarters.

The Government then prepared a search warrant, which the Magistrate Judge signed at 4:40 a.m. on January 19, 2017. (*Id.* at PageID #364–65.) The ensuing search of Defendant's laptop revealed evidence of Fruitfly and child pornography produced by the unauthorized Fruitfly recordings. (*Id.* at PageID #365.) The Government subsequently obtained a warrant to search Defendant's work computer, and Defendant later confessed to the crimes. (Mot to. Suppress at PageID #241–42, ECF No. 63; Resp. in Opp'n at PageID 365, ECF No. 66.) The Government arrested Defendant on January 25, 2017, pursuant to a criminal complaint. (Complaint, ECF No. 1.)

Defendant filed the instant Motion to Suppress on April 28, 2019. (ECF NO. 63.) He claims the Government's warrantless search and seizure on January 18, 2017, violated the Fourth Amendment and, therefore, all evidence obtained from his personal laptop and external hard drive must be suppressed. (*Id.* at PageID #236.) Defendant also seeks to suppress "all other derivatively obtained evidence," including "derivatively resulting statements" he made and data from his work computer and flash drive. (*Id.*) The Government responds that suppression is unwarranted because the events on January 18, 2017, were lawful and justified by the imminent threat of evidence destruction. (Resp. in Opp'n at PageID #366–79, ECF No. 66.) Further, the Government argues that the FBI agents acted in good faith and inevitably would have discovered the allegedly tainted evidence. (*Id.* at PageID #380–85.) The court held a two-day suppression hearing beginning on December 9, 2019, with respect to Defendant's Motion.

II. LEGAL STANDARD

The Fourth Amendment protects against unreasonable searches and seizures by generally forbidding the introduction in court of evidence obtained by government officers through a violation of the Amendment. *Olmstead v. United States*, 277 U.S. 438, 462 (1928). To safeguard this right, evidence secured through an illegal search or seizure may not be used in criminal proceedings. *Mapp v. Ohio*, 367 U.S. 643 (1961). Although the Fourth Amendment "contains no provision expressly precluding the use of evidence obtained in violation of its commands," the exclusionary rule "operates as 'a judicially created remedy . . . through its deterrent effect, rather than a personal constitutional right of the party aggrieved.'" *United States v. Leon*, 468 U.S. 897, 906 (1984) (quoting *United States v. Calandra*, 414 U.S. 338, 348 (1974)).

It is well-settled under the Fourth Amendment "that a search conducted without a warrant issued upon probable cause is 'per se unreasonable . . . subject only to a few specifically established and well-delineated exceptions.'" *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973) (citations omitted). As relevant here, warrantless searches are permissible when police have consent to conduct a search and when certain exigencies exist, such as the need to preserve evidence. *See Bustamonte*, 412 U.S. at 219 (upholding warrantless search conducted pursuant to consent); *Illinois v. McArthur*, 531 U.S. 326, 334 (2001) (upholding exigency-based seizure conducted without a warrant).

III. LAW AND ANALYSIS

Defendant seeks to suppress all evidence stemming from the warrantless seizure of his laptop. His Motion identifies several potential violations of the Fourth Amendment: First, Defendant argues that the Government agents used coercive tactics to pressure his parents into giving consent to enter and search the home. Because his parents' consent was involuntary, Defendant argues, the subsequent search violated the Fourth Amendment. Second, even if the agents had consent to enter the home, Defendant asserts that his parents did not have authority to let the agents enter and search

his computer room. Finally, Defendant argues that the agents violated his Fourth Amendment rights by searching and seizing his laptop without consent. The Government counters that the agents conducted their search pursuant to valid consent and that, in any event, their actions were justified by exigent circumstances. The court addresses the Government's asserted justifications—consent and exigency—in turn. Further, although the court's finding that exigent circumstances justified the agents' actions is dispositive, the court finds that suppression is not warranted even if no exigent circumstances existed because exceptions to the exclusionary rule apply in this case.

A. Consent

A warrantless search does not violate the Fourth Amendment if police conduct the search pursuant to valid consent. *See Bustamonte*, 412 U.S. at 219. To satisfy this warrant exception, the Government must present "clear and positive testimony" that the consent was "unequivocally, specifically, and intelligently given, uncontaminated by any duress and coercion." *United States v. Tillman*, 963 F.2d 137, 143 (6th Cir.1992). The Sixth Circuit has held that "[w]hether consent is voluntary is a question of fact determined from the totality of the circumstances." *United States v. Tatman*, 397 F. App'x 152, 164 (6th Cir. 2010) (quoting *United States v. Lopez–Medina*, 461 F.3d 724, 737 (6th Cir.2006)). Relevant factors in this determination include "the defendant's age, intelligence, and education; whether he understands his constitutional rights; the length and nature of the detention; and the use of coercive or punishing conduct by the police." *United States v. Valdez*, 147 F. App'x 591, 596 (6th Cir. 2005) (citing *United States v. Jones*, 846 F.2d 358, 360 (6th Cir.1988)). In weighing these factors, courts look for "indications of 'more subtle forms of coercion that might flaw [an individual's] judgment.'" *United States v. Cochrane*, 702 F.3d 334, 342 (6th Cir. 2012) (quoting *United States v. Watson*, 423 U.S. 411, 424 (1976)).

Even when an individual voluntarily consents to a search, however, Government agents violate the Fourth Amendment if their search exceeds the scope of consent or if the consenting

individual did not have authority over the area or property searched. The standard for measuring the scope of consent is objective reasonableness—*i.e.* what the typical reasonable person would have understood by the exchange between police officers and the person giving consent. *See Florida v. Jimeno*, 500 U.S. 248, 252 (1991). In the case of co-habitants, police may get consent from "an occupant who shares, or is reasonably believed to share, authority over the area in common with a co-occupant who later objects to the use of evidence so obtained." *Georgia v. Randolph*, 547 U.S. 103, 106 (2006).

1. Coercion and Voluntariness of Parents' Consent

Defendant asserts that the Government agents coerced his parents into giving consent to enter and search the house. (Mot. to Suppress at PageID #249–51, ECF No. 63.) Defendant repeatedly emphasizes that the FBI never gave his parents "a complete explanation of their rights and options" to refuse the agents' requests. (*Id.* at PageID #250.) He argues that this failure, combined with the circumstances surrounding the events and the agents' subtly coercive tactics, rendered his parents' consent involuntary. (*Id.*)

As an initial matter, the court notes that Defendant lacks standing to challenge the voluntariness of his parents' consent. It is well-settled that "Fourth Amendment rights are personal rights" that "may not be vicariously asserted." *United States v. Noble*, 762 F.3d 509, 526 (6th Cir. 2014) (quoting *Alderman v. United States*, 394 U.S. 165, 174 (1969)). That means, "for a defendant to argue successfully that evidence should be suppressed, he must show, as an element of his claim, that the government infringed upon *his* Fourth Amendment rights." *Noble*, 762 F.3d 509 at 526 (emphasis added). Consequently, Defendant cannot challenge the voluntariness of his parents' consent because the alleged coercion implicates *their* Fourth Amendment rights, not Defendant's.

But even if Defendant could vicariously assert his parents' Fourth Amendment rights, the record does not show that his parents' consent was contaminated by coercion of the agents. Nothing

suggests that Mr. and Mrs. Durachinsky's age, intelligence, or education undermined their ability to give informed consent. To the contrary, they consented to searches of their own computers but refused to let the agents search Defendant's laptop. This demonstrates familiarity with and understanding of their rights under the Fourth Amendment. *See United States v. Worley*, 193 F.3d 380, 387 (6th Cir. 1999) ("[K]nowledge of the right to refuse consent is one factor to be taken into account." (quoting *Bustamonte*, 412 U.S. at 227)). At the hearing, the Government also clearly established that the FBI agents were polite and respectful throughout their interactions with Defendant's parents. In fact, Mrs. Durachinsky admitted that the agents never raised their voices, made threats, or looked in areas of the house without permission. Accordingly, the court finds that Mr. and Mrs. Durachinsky voluntarily consented to let the agents enter the home and search various rooms.[1]

2. Consent and Common Authority over Defendant's Computer Room

Defendant next argues that the agents lacked authority to enter his computer room, even if they had consent to search other parts of the house. (Mot. to Suppress at PageID #251–52, ECF No. 63.) In his Motion, Defendant claims that the Government failed "to show that any consent to enter various parts of [the Durachinsky's] home . . . extended to Defendant's computer room." (*Id.* at PageID #252.) Alternatively, Defendant also seems to suggest that his parents lacked authority over the computer room because the room "was used exclusively by Defendant," which means any consent his parents gave would be invalid. (*Id.* at PageID #240.)

---

[1] Still, the court is not blind to the intimidation inherent in a knock and talk, especially one that involves FBI agents arriving late at night to investigate criminal activity allegedly linked to the individual's home address. It likely would have been less threatening had the agents arrived at a more reasonable hour and more explicitly notified Defendant's parents that they would not be penalized if they refused to cooperate. But while the court is sympathetic to the unwelcome situation the Government thrust upon Mr. and Mrs. Durachinsky, the law and facts do not support a finding that their consent was involuntary.

Defendant's first argument—that his parents never gave consent to search the computer room—fails. As Mrs. Durachinsky testified at the hearing, the agents entered the house calmly and explained the purpose of their visit while seated around the Durachinsky's kitchen table. After Defendant's parents agreed to sign consent to search forms for their respective computers, Mr. Durachinsky took agents to see his computer in the basement and Mrs. Durachinsky showed them her laptop in the living room. The agents then asked if there were other computers in the home, and Mrs. Durachinsky told them Defendant's laptop was in another room. At the agents' request, she led them down the hall from the living room to Defendant's computer room, opened the door, and pointed to Defendant's laptop on a desk.[2] (*See id.*) Defendant's parents never told the agents to stay out of the computer room or otherwise indicated that the room was off-limits. And again, as Mrs. Durachinsky confirmed, the agents never raised their voices, made threats, or acted disrespectfully. Under these circumstances, an objectively reasonable person would interpret the parents' actions as giving consent to enter the room. Indeed, as the Sixth Circuit has explained, as long as the interaction is untainted by coercion, duress, or trickery, if police properly request permission to enter and an individual responds by stepping aside or opening a door, the non-verbal action conveys valid consent. *See United States v. Carter*, 378 F.3d 584, 587–88 (6th Cir. 2004) (en banc) (holding police had consent where they asked permission and defendant "stepped back and cleared a path for the officers to enter"). Because the agents did not coerce Defendant's parents, as discussed above, the court finds that Mr. and Mrs. Durachinsky voluntarily consented to a search of the computer room.

The question remains, however, whether Defendant's parents had authority to let the agents into the computer room. The Supreme Court has said that a warrantless search does not violate the

---

[2] Mrs. Durachinsky could not recall whether she or her husband opened the door to the computer room. This detail makes no difference because, either way, their actions conveyed consent to enter the room.

Fourth Amendment if law enforcement officers receive consent to search "from a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected." *United States v. Matlock*, 415 U.S. 164, 171 (1974). The term "common authority" refers to the "mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched." *Id.* at 171 n.7; *see also Randolph*, 547 U.S. at 110. Moreover, it is well-established that "[t]he police may also search a residence with the permission of an occupant whom they reasonably, even if erroneously, believe to have authority to consent to the search." *Pratt v. United States*, 214 F. App'x 532, 535 (6th Cir. 2007) (citing *Illinois v. Rodriguez*, 497 U.S. 177, 186 (1990)). In other words, "[s]o long as the consenting individual has actual common authority over the room . . . or apparent common authority over the room, . . . officers may rely on the consent." *United States v. Caldwell*, 518 F.3d 426, 429 (6th Cir. 2008) (citing *Matlock*, 415 U.S. at 170–71; *Rodriguez*, 497 U.S. at 181).

In the Sixth Circuit, courts generally presume that family members share common authority over the entire family residence unless one member "has clearly manifested an expectation of exclusivity" over a particular room. *United States v. Clutter*, 914 F.2d 775, 777–78 (6th Cir. 1990). In addition to any steps taken to maintain privacy—such as locked doors or an agreement to enter only with permission—courts consider "whether the co-occupant owns the residence or is named on the lease; if the individual contributed rent; and whether the individual visited the residence when the co-occupant was not present." *Pratt*, 214 F. App'x at 535 (citing *Rodriguez*, 497 U.S. at 181); *see also United States v. Gillis*, 358 F.3d 386, 391 (6th Cir. 2004) (holding that girlfriend had apparent authority to consent because she was named on lease, even though she did not have keys to the apartment).

In light of these factors, the court concludes that Mr. and Mrs. Durachinsky had common authority over Defendant's computer room. Defendant asserts that the computer room "was used exclusively by Defendant," (Mot. to Suppress at PageID #240, ECF No. 63), but the record shows otherwise. At the hearing, Mrs. Durachinsky testified that she and her husband used the room for extra storage. Morever, there is no evidence that the room was ever locked or that Defendant's parents had an agreement with Defendant to enter the computer room only with his consent. *See Pratt*, 214 F. App'x at 535; *see also United States v. Rith*, 164 F.3d 1323, 1331 (10th Cir. 1999). To the contrary, Mr. and Mrs. Durachinsky's actions reflect that they had unrestricted access to the computer room—even if they seldom entered it. Finally, the court notes that Defendant's parents own the house and, while the record does not indicate whether Defendant paid rent, Mrs. Durachinsky told the agents that Defendant lived there only part of the week. (*See* Resp. in Opp'n at PageID #363, ECF No. 66.) Collectively, these facts establish that Defendant's parents had actual authority over the computer room. But even if they lacked actual authority, Mr. and Mrs. Durachinsky conveyed apparent common authority. The agents reasonably concluded that the parents' control extended to the computer room, and there was no reason to suspect otherwise. *See Randolph*, 547 U.S. at 112 (holding that police have no burden "to eliminate the possibility of atypical arrangements, in the absence of reason to doubt that the regular scheme was in place"). Because the record shows that Mr. and Mrs. Durachinsky had actual, or at least apparent, authority over the computer room, the court finds that the agents justifiably relied on the consent they received.

3. Defendant's Laptop

Finally, Defendant maintains that the FBI agents did not have valid consent to search or seize his laptop, which the agents discovered in the computer room. This argument is persuasive. As the Sixth Circuit explained in *United States v. Waller*, 426 F.3d 838 (6th Cir. 2005), consent to search

a building or a particular room does not necessarily extend to closed containers or objects discovered inside that building or room. *See id.* at 845. Rather, "valid consent to search the closed container must come from one who has common authority over the effects sought to be inspected." *Id.* (citing *United States v. Karo*, 468 U.S. 705, 715 (1984)).

Here, the agents obviously lacked consent to search Defendant's laptop. That the agents sought and received signed consent forms before searching Mr. and Mrs. Durachinsky's computers shows that they recognized the need for specific consent to search electronic devices within the home even though they already received consent to enter the house and the computer room. Further, the agents knew Defendant was an adult, that he was the owner and exclusive user of the ACER Aspire laptop, and that the laptop was in a separate room. *See United States v. Trejo*, 471 F. App'x 442, 448 (6th Cir. 2012) ("[A]pparent authority is established by features like location and use."). Regardless, no ambiguity remained after Mrs. Durachinsky expressly refused to let the agents search Defendant's laptop without Defendant's consent—just as Defendant refused to give consent when talking to SA Florence on the phone later. These facts allow only one conclusion: the Government had no authority, actual or apparent, to search Defendant's laptop.

Nonetheless, the Government argues that the agents did not violate the Fourth Amendment because they did not search the laptop until after they acquired a warrant. (*See* Resp. in Opp'n at PageID #377, ECF No. 66.) At the suppression hearing, CS Corrigan testified that he ran commands to check whether Defendant's laptop was encrypted after he initially encountered the device. CS Corrigan also maintained that he conducted his sweep for encryptions without accessing any files or user data on the laptop. Importantly, there is no evidence to refute this assertion.

To determine whether a search occurred, courts look to whether there was a property-based trespass or whether the individual held a reasonable expectation of privacy. *See Florida v. Jardines*, 569 U.S. 1, 7–10 (2013) (holding that deploying police dog to sniff front porch is a search); *Riley*

v. California, 573 U.S. 373, 391–97 (2014) (holding that individuals maintain expectation of privacy in cell phones during an arrest). In this case, the court finds that police conducted a search under either analytical framework. Physical manipulation—*i.e.* pressing buttons on the keyboard and "interrogat[ing] the code" on the laptop—constitutes a search in the literal sense. *See United States v. Correa*, 908 F.3d 208, 217 (7th Cir. 2018); *see also Arizona v. Hicks*, 480 U.S. 321, 325 (1987) ("A search is a search, even if it happens to disclose nothing but the bottom of a turntable."). Moreover, a layperson almost certainly would construe such actions as an invasion of privacy. *See Jardines*, 569 U.S. at 9 (noting with concern conduct that "would inspire most of us to—well, call the police").

But a search does not violate the Constitution if it was reasonable, meaning "it falls within a specific exception to the warrant requirement." *Riley*, 573 U.S. at 382. The Supreme Court has explained that it determines whether a particular type of search is exempt from the warrant requirement "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Id.* at 385 (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)). When it comes to modern technology, courts recognize that the nature of electronic devices "greatly increases the potential privacy interests at stake." *United States v. Lichtenberger*, 786 F.3d 478, 488 (6th Cir. 2015). Yet the search at issue here does not necessarily implicate those weighty privacy interests because the agents did not attempt to open or otherwise access any personal data on Defendant's laptop. Instead, they merely checked the laptop for encryption and found it unlocked and unprotected. *Contra Riley*, 573 U.S. at 389 (scoffing at encryption-based argument because "[l]aw enforcement officers are very unlikely to come upon such a [device] in an unlocked state").

In any event, as discussed in more detail below, the court finds that the exigent circumstances exception applies. At the hearing, CS Corrigan testified that the check for encryptions was necessary

to prevent evidence on the laptop from being destroyed. In other words, the agents already had determined that exigent circumstances justified seizing the laptop, and they were taking steps to ensure the preservation of data during the seizure. *See id.* at 402 (discussing "the availability of the exigent circumstances exception"). The Government produced evidence that this practice is "standard procedure for seizing any computer that is powered on." (Resp. in Opp'n at PageID #373 n.7, ECF No. 66 (citing Ovie Carroll, *Challenges in Modern Digital Investigative Analysis*, 65 U.S. Atty's Bull. 25, 27–28 (January 2017).) As the Supreme Court recognized in *Riley*, when law enforcement officials encounter an electronic device, they can take reasonable measures to prevent loss of data without running afoul of the Fourth Amendment. *See Riley*, 573 U.S. at 390–91 (explaining police can "turn the [device] off or remove its battery," place the device in an enclosure that blocks signal transmission, or disable the device's "automatic-lock feature in order to prevent the phone from locking and encrypting data"). Given the pressing need to preserve evidence and the limited intrusion on Defendant's privacy interests caused by CS Corrigan's search for encryption, the court finds that the agents' actions were reasonable.

B. Exigent Circumstances

The Sixth Circuit has identified three key factors to determine if a warrantless seizure is lawful: (1) there must be probable cause, (2) there must be an exigent circumstance, and (3) the seizure must be sufficiently limited in scope and timing. *See United States v. Bradley*, 488 F. App'x 99, 101 (6th Cir. 2012); *see also McArthur*, 531 U.S. at 331–33. The court addresses each of these factors in turn.

1. Probable Cause

In the Sixth Circuit, "[t]he probable cause requirement . . . is satisfied if the facts and circumstances are such that a reasonably prudent person would be warranted in believing that an offense had been committed and that evidence thereof would be found on the premises to be

searched." *Green v. Reeves*, 80 F.3d 1101, 1106 (6th Cir. 1996) (quotation omitted). With regard to cybercrime, probable cause to search a residence exists if an IP address associated with the criminal activity resolves to that address. *See United States v. Hinojosa*, 606 F.3d 875 (6th Cir. 2010); *United States v. Gillman*, 432 F. App'x 513 (6th Cir. 2011).

Here, the FBI had probable cause to search Defendant's residence and the computers located there. First, CWRU informed the Government that it had connected Defendant's alumni email account to an IP address associated with Fruitfly. Second, from AT&T's subpoena responses, the Government determined that the IP address resolved to Defendant's residence. Third, the articles publicizing Fruitfly identified an IP address traceable to Defendant. Finally, CWRU informed the FBI that Defendant had been disciplined for hacking the school's network while he was a student. (Resp. in Opp'n at PageID #360–61, ECF No. 66); *see also United States v. Dryer*, 580 F.3d 386, 392 (6th Cir 2009) (holding that criminal history is relevant to the probable cause inquiry). These facts were sufficient to establish probable cause before the agents arrived at Defendant's home. Moreover, after the agents arrived at the Durachinsky residence but before they entered the computer room or seized Defendant's laptop, the agents lawfully obtained additional information that further established probable cause, including Mrs. Durachinsky's statements regarding Defendant's computer savvy and his history of hacking.

2. Exigency

In the Sixth Circuit, the "urgent need to prevent evidence from being lost or destroyed" can justify a warrantless seizure of a laptop. *Bradley*, 488 F. App'x at 103. There are two steps to the exigency analysis in this context. First, the Government must show "an objectively reasonable basis for concluding that the loss or destruction of evidence is imminent." *Id.* (quoting *United States v. Sangineto-Miranda*, 859 F.2d 1501, 1512 (6th Cir.1988)). Second, the court then weighs "the

governmental interest being served by the intrusion against the individual interest that would be protected if a warrant were required." *United States v. Plavcak*, 411 F.3d 655, 664 (6th Cir. 2005).

As to the first part of the analysis, several factors support finding an exigent circumstance. First, it is objectively reasonable to believe that someone with Defendant's technological savvy and sophistication would have noticed, read, and reacted to the two articles published on January 17, 2017. Second, Defendant had recently moved the Fruitfly infrastructure to a new IP address, which suggests he actively monitored the malware and would be responsive to victims' remediation efforts. With this in mind, it was reasonable for the FBI agents to believe "that [Defendant] would destroy evidence of his crimes." (Resp. in Opp'n at PageID #372, ECF No. 66.) Finally, the Government asserts that the security patch Apple produced for its users would have eliminated the Fruitfly network and destroyed crucial evidence. Because Apple had already begun rolling out the security update, the threat of losing evidence loomed large.

However, several factors cut against the Government's exigency argument. In particular, the court notes that several hours elapsed between the time the articles were published and the time agents arrived at Defendant's home. (*See* Ex. to Resp. in Opp'n at PageID #392, ECF No. 66-1.) One could interpret this delay as showing a lack of urgency regarding the threat of imminent evidence destruction. The delay is all the more noticeable because it did not take long for the Government to apply for and receive a search warrant later that night. However, the Government argued at the suppression hearing that there were valid reasons for the delay. SA Florence testified that, after the articles appeared online, the FBI agents engaged in extensive conversations with lawyers from the United States Attorney's Office and the Department of Justice to determine the best course of action. Ultimately, the Government concluded that more legal process was necessary before seeking a warrant and that the agents should conduct a knock and talk in the meantime due to the significant threat of evidence destruction.

After considering the facts and all relevant factors, the court concludes that Apple's security patch and the publication of the two articles earlier in the day provided "an objectively reasonable basis" for the FBI agents to conclude that evidence loss or destruction was imminent. *See Bradley*, 488 F. App'x at 103. Though the Government's decision to wait for a period of time before moving on Defendant's residence or seeking a warrant raises questions, the court ultimately accepts as true the Government's assertion that the delay resulted from an abundance of caution as the agents discussed the legality of their options. The threat of losing evidence was as urgent at 10:00 p.m. as it had been earlier in the day, and the Government should not be penalized for taking additional time in an attempt to ensure its investigation complied with the law. Accordingly, the court finds that the events earlier in the day created exigent circumstances.

That means, as the Government argues, that probable cause and exigent circumstances existed *before* the FBI agents arrived at Defendant's home. (*See* Resp. in Opp'n at PageID #362, ECF No. 66 ("[T]he [Government] does not rely on any events that took place at [Defendant's] home to establish either probable cause or exigent circumstances").) The parties spent a great deal of time at the suppression hearing arguing whether Defendant's laptop was open or closed when the agents first encountered it. Given the testimony and report from Defendant's computer expert and the FBI's own technical report, which contradicts the testimony of the agents, the court finds that the preponderance of the evidence suggests the laptop was closed and the screen was blank when agents arrived at the Durachinsky's home. However, the physical state of the laptop does not directly impact the court's Fourth Amendment exigency analysis because the exigent circumstance arose earlier in the day before the knock and talk occurred. The urgency only intensified after the agents arrived at the Durachinsky's house, learned of Defendant's computer, and discovered that Defendant could control it remotely.

Turning to the second part of the exigency analysis, the court also finds that the Government's interest in seizing Defendant's laptop outweighed the individual interest in requiring the Government to get a warrant. The Sixth Circuit has explained that "the governmental interest in protecting evidence from destruction is particularly high where digital evidence is involved, because such evidence is inherently ephemeral and easily destructible." *Bradley*, 488 F. App'x at 104. Further, although the Government did not yet know the malware had captured explicit images of minors, the Government did know that Fruitfly represented a grave threat to the weighty privacy interests of its victims. *See Frisby v. Schultz*, 487 U.S. 474, 484 (1988) ("The State's interest in protecting the well-being, tranquility, and privacy of the home is certainly of the highest order." (quoting *Carey v. Brown*, 447 U.S. 455, 471 (1980))). Finally, the Government's seizure primarily implicated Defendant's property interests rather than his privacy interests. As discussed earlier, the Government's unrefuted testimony at the suppression hearing established that the agents limited their initial search to checking for encryptions. The Government did not conduct a comprehensive search of the laptop until later, after obtaining a search warrant. Given these considerations, the court finds that the Government's interests outweighed the individual interest at stake.

3. Scope and Timing

Although the Government established that exigent circumstances justified its warrantless seizure of Defendant's laptop, the court also must analyze whether the agents conducted the seizure in a reasonable manner. Courts measure reasonableness in this context by examining the totality of the circumstances. *Bradley*, 488 F. App'x at 105 (citing *Randolph*, 547 U.S. at 125; *Ohio v. Robinette*, 519 U.S. 33, 39 (1996)).

Ultimately, the court finds that the scope and timing of the Government's actions were not inappropriate or unreasonable. At the hearing, Defendant's counsel repeatedly emphasized that the FBI agents arrived at the Durachinsky home around 10:00 p.m. on a cold, January night; that

Defendant's parents were in bed when the agents arrived; that Mr. and Mrs. Durachinsky are in their sixties and live in a small home; and that it was intimidating for so many agents to approach and enter the home. But while it may have been less threatening for the agents to arrive earlier in the day, the agents gave a credible explanation as to why they conducted the knock and talk that evening. Further, the record suggests that the agents acted as quickly as possible; they were polite and tried to minimize the intrusion on Defendants' parents; they did not pressure Defendant's parents or move around the house without permission; they seized Defendant's laptop and hard drive only; they sought a warrant immediately after the knock and talk and obtained it within a reasonable time (less than six hours); and they did not conduct a comprehensive search of the laptop until they had the warrant in hand. As for the month and the weather, those factors were beyond the Government's control.

Moreover, once Defendant knew about the investigation, the agents could not leave the laptop at the Durachinsky's house unguarded. Courts long have doubted the wisdom of leaving easily destructible contraband in the owner's possession once the owner is aware of an investigation. *See McArthur*, 531 U.S. at 332. This issue tends to arise in drug cases, but courts including the Sixth Circuit have begun to apply the same logic to computers. *See Bradley*, 488 F. App'x at 103. Of course, the FBI agents could have remained at the Durachinsky's house all night to guard the laptop and prevent any tampering. But "that, too, would have implicated Fourth Amendment concerns." *Id.* at 105 (citing *Segura v. United States*, 468 U.S. 796, 809 (1984)).

The Supreme Court's observation in *United States v. Sharpe*, 470 U.S. 67 (1985), is instructive here:

> A creative judge engaged in post hoc evaluation of police conduct can almost always imagine some alternative means by which the objectives of the police might have been accomplished. But the fact that the protection of the public might, in the abstract, have been accomplished by less intrusive means does not, itself, render the

> search unreasonable. The question is not simply whether some other alternative was available, but whether the police acted unreasonably in failing to recognize or to pursue it.

Id. at 686–87. While the Government could have done things differently to reduce the disruption on Defendant and his parents, the court finds that the agents did not act unreasonably in carrying out the knock and talk or the subsequent seizure of Defendant's laptop.

C. Exclusionary Rule and Exceptions

Even assuming there was no exigent circumstance to justify the Government's warrantless search and seizure of Defendant's laptop, that does not mean suppression is required. *See Herring v. United States*, 555 U.S. 135, 137 (2009) ("[S]uppression is not an automatic consequence of a Fourth Amendment violation.") In *Herring*, the Supreme Court explained that, "the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Id.* at 144. Thus, "[t]o trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.*

Although Defendant does not explicitly challenge the facial validity of the Government's search warrant, he urges the court to suppress all evidence as poisoned fruit flowing from the allegedly tainted initial search and seizure of his laptop. (Mot. to Suppress at PageID #236–37, 248, ECF No. 63.) The Government responds that, even if the initial search and seizure was unlawful, three well-established exceptions to the exclusionary rule apply in this case: the inevitable discovery doctrine, the independent source doctrine, and the good-faith exception. (Resp. in Opp'n at PageID #380–85, ECF No. 66.) After considering the parties' arguments, the court finds that the inevitable discovery and independent source doctrines apply, but the good-faith exception does not.

The inevitable discovery exception applies if evidence obtained through an unlawful search "inevitably would have been acquired through lawful means had the government misconduct not

occurred." *United States v. Kennedy*, 61 F.3d 494, 497 (6th Cir. 1995); *see also United States v. Chapman-Sexton*, 758 F. App'x 437, 441 (6th Cir. 2018) ("[T]he inevitable-discovery exception 'applies when . . . evidence discovered during an illegal search would have been discovered during a later legal search and the second search inevitably would have occurred in the absence of the first.'" (quoting *United States v. Keszthelyi*, 308 F.3d 574 (6th Cir. 2002))). Although speculation must be kept to a minimum, "[t]he exception requires the district court to determine, viewing affairs as they existed at the instant before the unlawful search, what would have happened had the unlawful search never occurred." *Kennedy*, 61 F.3d at 498 (quoting *United States v. Eng*, 971 F.2d 854, 861 (2d Cir.1992)). For example, the Sixth Circuit has recognized that discovery is inevitable "when the government can demonstrate *either* the existence of an independent, untainted investigation that inevitably would have uncovered the same evidence or other compelling facts establishing that the disputed evidence inevitably would have been discovered." *Keszthelyi*, 308 F.3d at 574. The Government has made that showing here. In the moment immediately before the allegedly unlawful search and seizure of Defendant's laptop, the Government had amassed a substantial body of evidence implicating Defendant. Armed with this information, the court finds that the Government could and would have obtained a search warrant. Indeed, the Government had already taken initial steps to get a warrant before going to the Durachinsky's house. (Resp. in Opp'n at PageID #382, ECF No. 66.)

Similarly, the independent source doctrine allows courts to admit "evidence initially discovered during, or as a consequence of, an unlawful search, but later obtained independently from activities untainted by the initial illegality." *Murray v. United States*, 487 U.S. 533, 537 (1988). Under this exception, even if police include unlawfully obtained information in a search warrant affidavit, evidence obtained later pursuant to the warrant is admissible as long as the "independent and legitimately obtained evidence" is sufficient to establish probable cause. *See United States v.*

Jenkins, 396 F.3d 751, 759–60 (6th Cir. 2005) (citations omitted); *see also United States v. Gibson*, No. 1:13-CR-49, 2013 WL 11816820, at *9 (N.D. Ohio Aug. 30, 2013). Here, the affidavit included more than enough legitimately obtained information to establish probable cause. In addition to the wealth of evidence the Government lawfully collected before the knock and talk, the Government also lawfully learned from Defendant's parents that Defendant had an extensive history of hacking-related offenses, that his laptop was at the house, and that Defendant could access it remotely. Consequently, even after scrubbing any allegedly tainted information from SA Macfarlane's affidavit—that the laptop lid was open, that there was movement on the screen, and that a malware control panel was visible—the subsequently issued search warrant still would be valid. *See Hinojosa*, 606 F.3d at 885 (6th Cir.2010) (finding warrant valid, despite potentially illegally obtained information in the affidavit, because suspected IP address corresponded to defendant's home). Thus, the evidence the Government obtained pursuant to the search warrant, which encompasses everything they learned through the allegedly unlawful search, was "independent" of any potential Fourth Amendment violation and, therefore, need not be suppressed.

The good-faith exception, however, does not apply. This exception recognizes that suppressing evidence serves little deterrent effect "when the police act with an objectively 'reasonable good-faith belief' that their conduct is lawful . . . or when their conduct involves only simple, 'isolated' negligence." *Davis v. United States*, 564 U.S. 229, 238 (2011) (citing *Leon*, 468 U.S. at 909; *Herring*, 555 U.S. at 142). Typically, this exception "is inapplicable where a warrant was secured in part on the basis of an illegal search or seizure." *United States v. Davis*, 430 F.3d 345, 358 n.4 (6th Cir. 2005). But the Sixth Circuit has recognized a narrow exception for cases in which "the facts surrounding the initial Fourth Amendment violation were 'close enough to the line of validity'" to make the police officer's conduct objectively reasonable. *United States v. McClain*, 444 F.3d 556, 566 (6th Cir. 2005); *but see United States v. Tucker*, 742 F. App'x 994, 1003 (6th Cir.

2018) (distinguishing *McClain*). Such borderline cases are uncommon, however. *See Tucker*, 742 F. App'x at 1003 ("The question before us, therefore, is whether 'this is one of those *unique* cases in which the *Leon* good[-]faith exception should apply despite an earlier Fourth Amendment violation.'" (quoting *McClain*, 444 F.3d at 565)). The court is not convinced this is one of those rare cases, especially in light of the court's finding that the agents' testimony regarding the physical state of Defendant's laptop (*i.e.* that it was open and movement was visible on the screen) was contradicted by Defendant's expert and the FBI's own technical report. Accordingly, the court finds that, if the initial search and seizure were unconstitutional, the good-faith exception does not insulate evidence the Government obtained through subsequent searches.

IV. CONCLUSION

In sum, the court finds that Defendant's parents gave valid consent for the FBI agents to enter the home and search various rooms, such as the basement and computer room, and that the imminent threat of evidence destruction justified the Government's warrantless seizure of Defendant's laptop. But even if the Government's actions were found to be in violation of the Fourth Amendment, suppression is not warranted because the inevitable discovery and independent source doctrines apply. Therefore, for the foregoing reasons, the court denies Defendant's Motion to Suppress (ECF No. 63).

IT IS SO ORDERED.

/s/ SOLOMON OLIVER, JR.
UNITED STATES DISTRICT JUDGE

April 30, 2020